Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Tarea 3: Modelos de clasificación

Aprendizaje Automático

Nombre: Sergio Andrés Elizondo Rodríguez

Grupo: 003

Maestro: José Anastacio Hernández Saldaña

Sábado 20 de Julio del 2024

Introducción

NSL-KDD es un conjunto de datos ampliamente utilizado en la investigación de sistemas de detección de intrusiones (*IDS*, por sus siglas en inglés). Está compuesto por registros de tráfico de red, con características que describen cada conexión, y su etiqueta correspondiente, la cual indica si la conexión es normal o se trata de un ataque.

El análisis realizado en el presente reporte busca evaluar diferentes modelos de clasificación para identificar el mejor enfoque con el fin de distinguir entre conexiones normales y ataques. El objetivo es seleccionar el modelo que mejor represente los datos y ofrezca un rendimiento robusto, para lo cual se realiza un ajuste de hipeparámetros y se comparan múltiples técnicas de clasificación.

Procesamiento previo

Antes de aplicar los modelos, se realizó un procesamiento previo para garantizar que las variables sometidas a análisis fueran las adecuadas; en particular, se aplicaron dos tratamientos diferentes:

- **Variables categóricas:** Representan categorías o grupos discretos (como el tipo de conexión). Se convirtieron en representaciones binarias utilizando *OneHotEncoder* para poder usarlas en los modelos de regresión.
- **Variables numéricas:** Representan datos cuantitativos (como las métricas de tráfico de red). Se normalizaron para que fueran compatibles con todos los modelos.

Modelos

Para garantizar una evaluación robusta, se implementó una búsqueda de hiperparámetros en cuadrícula (*grid search*) con validación cruzada (*KFold*), seleccionando los parámetros que maximicen la sensibilidad (*recall*). Se decidió utilizar esta métrica ya que en este estudio es esencial clasificar correctamente los positivos (datos que representan un ataque) y, por lo tanto, minimizar los falsos negativos. Se utilizó un muestreo de 400 elementos para reducir el tiempo de búsqueda.

A continuación, se presentan los modelos aplicados y los resultados obtenidos:

Modelo	Sensibilidad	Mejores parámetros
***K* vecinos más cercanos**	0.9289	3 vecinos Ponderación por distancia
Regresión logística	0.9538	C = 10, Penalización L2
Máquinas de vectores de soporte (SVM)	0.9559	C = 100, Núcleo radial (*rbf*)
Árbol de decisión	0.9615	Profundidad máxima: 7 Mínimo de muestras por hoja: 1 Mínimo de muestras por división: 2

Potenciación de gradiente (*gradient boosting*)	0.9842	Tasa de aprendizaje: 0.1 Profundidad máxima: 4 Mínimo de muestras por hoja: 1 Mínimo de muestras por división: 2 Número de estimadores: 100
Bosque aleatorio	0.9842	Profundidad máxima: Por defecto Máximo de características: Por defecto Mínimo de muestras por hoja: 1 Mínimo de muestras por división: 2 Número de estimadores: 200

Gradient boosting y el bosque aleatorio son los modelos con mejor sensibilidad, lo cual sugiere que pueden captar relaciones complejas entre las características del conjunto de datos y la variable objetivo.

Resultados

Para evaluar el desempeño de los modelos de clasificación en el conjunto de datos completo, se realizó una prueba utilizando el mejor modelo identificado en la optimización: el bosque aleatorio. A continuación, se presentan las métricas obtenidas:

Métrica	**Valor**	**Interpretación**
Exactitud (*accuracy*)	0.8038	El 80.38% de las predicciones del modelo coinciden con las etiquetas reales.
Precisión (*precision*)	0.9687	La proporción entre verdaderos positivos y positivos predichos es alta. Esto sugiere que cuando el modelo predice una intrusión (comportamiento anómalo) es bastante confiable.
Sensibilidad (*recall*)	0.6772	El modelo identifica correctamente el 67.72% de los casos de intrusión. Aunque es una buena tasa de verdaderos positivos, esto sugiere que el modelo no captura todos los casos de intrusión.
Métrica F1	0.7971	El modelo muestra un rendimiento equilibrado entre precisión y sensibilidad.

Área bajo la curva ROC (*AUC-ROC*)	0.8241	El modelo tiene una buena capacidad para diferenciar entre intrusiones y comportamiento normal, ofreciendo un desempeño decente en términos de clasificación binaria.

Bibliografía

- **Base de datos:** NSL-KDD. GitHub. Recuperado el 21 de julio de 2024, de https://github.com/topics/nsl-kdd